Hanseatic Governance: Understanding Blockchain as Organizational Technology

Miscione, Gianluca ; Goerke, Tobias ; Klein, Stefan ; Schwabe, Gerhard ; Ziolkowski, Rafael

Abstract: Blockchain technology provides a distributed ledger and is based on a logic of peer to peer authentication. It gained prominence with the rise of cryptocurrencies but provides a much broader field of possible applications. While it has been originally closely linked to a libertarian agenda rejecting organizations, its developments have illustrated that this ideological framing is being reversed in practice. Based on contrastive empirical cases, the purpose of our paper is to discuss blockchain as an organizational technology. Its peculiar mode of governance, which we name 'Hanseatic', needs to mediate between the fluidity typical of Free and Open Source Software development and the immutability that use organizations adopt blockchain for.

Hanseatic Governance: Understanding Blockchain as Organizational Technology

Completed Research Paper

Gianluca Miscione
University College Dublin
Ireland
gianluca.miscione@ucd.ie

Stefan Klein
University of Münster
Germany
stefan.klein@wi.uni-muenster.de

Gerhard Schwabe
University of Zürich
Switzerland
schwabe@ifi.uzh.ch

Tobias Maximilian Goerke
University of Münster
Germany
t_goer02@uni-muenster.de

Rafael Ziolkowski
University of Zürich
Switzerland
ziolkowski@ifi.uzh.ch

Abstract

Blockchain technology provides a distributed ledger and is based on a logic of peer to peer authentication. It gained prominence with the rise of cryptocurrencies but provides a much broader field of possible applications. While it has been originally closely linked to a libertarian agenda rejecting organizations, its developments have illustrated that this ideological framing is being reversed in practice. Based on contrastive empirical cases, the purpose of our paper is to discuss blockchain as an organizational technology. Its peculiar mode of governance, which we name 'Hanseatic', needs to mediate between the fluidity typical of Free and Open Source Software development and the immutability that use organizations adopt blockchain for.

Keywords: Blockchain, FOSS, organizational technology, governance, bazaar, Hanseatic League

Introduction

Money does not have backup copies, thus its governance is different from data's. The failure in understanding this basic difference in its far-reaching consequences has led key players in the cryptocurrencies and blockchain spaces to assume that the well-tested and very effective mode of governance that define Free and Open Source Software (FOSS) would have been enough to manage blockchains successfully. The main problem this article addresses is that FOSS, and related theorizations, have focused on software *design* and production[1], whereas blockchains are defined by authentication, which depends on and is shaped by *use* contexts. Thus, through contrastive cases, it is argued that the governance of blockchains needs a peculiar

[1] At best, FOSS is agnostic about software use. For example, its 'freedom 0' recites "The freedom to run the program as you wish, for any purpose" (https://www.gnu.org/philosophy/free-sw.en.html)

arrangement, which we named 'Hanseatic' after the coalition of cities that formed the League which defined Northern European economics and politics before modern states substituted alliances with the Rule of Law.

Over recent years Bitcoin – the largest blockchain to date – has gone through never-ending conflicts so harsh in modes and tone that FOSS never saw. Disinformation campaigns, silencing or defamation of opponents, and overloads of the network to make it unusable led to multiple gridlock situations, thus repeated 'forks' (i.e. independent and incompatible spin-offs) of this blockchain. Another illustration of the shortcomings of rejecting explicit organizational governance, often derogatorily equated to 'central authority', is the failure of the Decentralized Autonomous Organization (The DAO) and its assumption that governance functions can be reduced to contracts, instantiated then automated via smart contracts. Overall, those cases illustrate the limitations of the explanatory power of the Bazaar metaphor, which Raymond (1999a) put forward to characterize FOSS governance.[2] To frame the far-reaching theoretical ramifications of these empirical problems, we need to take a step back.

Online, all data used to be the same, there is no inherent difference between original and copy. Since reproduction and distribution of data have nearly zero marginal cost, scarcity of data has become a non-issue in recent decades. In other words, the non-exclusivity (one's use does not exclude everyone else's) of information goods like a novel or a song has become more difficult to restrict by regulating their supports (paper books or music CDs). This is a root cause of both major transformations of industries, starting with music, and novel organizational forms like FOSS and Wikipedia.[3] The inherent difficulty of containing data replication and distribution made information technologies effective in minimizing transaction cost (Demil and Lecocq 2006), but also ill-suited to provide money, which must be non-counterfeitable – thus inherently exclusive – without a 'central authority' acting as guarantor. In a nutshell, blockchains substitute 'external' organizations with technical immutability, thus dependability, of a ledger authenticated by its so-called miners.[4] Despite these design intentions, our final claim is that blockchains are suitably conceptualized as organizational technologies, whose apt mode of governance is 'Hanseatic'.

The blockchain bypasses non-scarcity of data and brings exclusivity of data via native authentication into the digital environment (Miscione et al. 2018). The novelty introduced by blockchain is the distributed mode of ledger's authentication vis-á-vis certifying organizations (i.e. 'central authorities') with own mechanisms of accreditation and auditing. Bitcoin proved the viability of digital scarcity by making all transactions public, clustering them in 'blocks', each sealed by 51% of the available computing power.[5] This means that a blockchain is simply an ever-expanding collection of timestamped blocks of transactions whose integrity is authenticated by a combination of technical and governance designs. Those ledgers locate each and every item and differentiate it from any other at any point in time. In practice, it makes no sense to copy items out of the ledger that authenticates their validity. It would be like handwriting '100 Euros' on a piece of paper hoping to buy something with it. Reversely, if a piece of data (like a novel for instance) retains its validity outside its blockchain, relying on a blockchain is pointless, if not impractical, in the first place.

Blockchain originated from the need that any currency has to avoid counterfeiting and has been subsequently applied to new domains like transaction records (of financial exchanges or supply chains, for example) or registries (vehicle records and cadasters, among others). This means that cryptocurrencies are authenticated tokens, which can be used by whomever accepts them, thus money's fungibility. The deployment of blockchains to specific domains like used cars and land registries (which we present below) requires to adjust to the specificities of each use context, which cuts fungibility (clearly, one cannot trade a car for a parcel directly even if their records were on the same blockchain, say Ethereum, which also runs a currency). Despite its origins rooted in the avoidance of organizations, seen as limiting the freedom of individuals, we

[2] It is noteworthy that, even if it is well established, the Bazaar metaphor (reminiscent of trades and haggling) is probably not the most appropriate to characterize FOSS.

[3] This text does not rely on differences between data and information. The main dichotomy here is data/information vs. tokens, i.e. blockchain-authenticated records.

[4] Authentication is here intended in its basic meaning of certification of genuinity, i.e. non-tempered with. *Per se*, the immutability of distributed ledgers does not guarantee data quality, even if transparency and traceability may deter from poor data entry.

[5] For space limitation, this article keeps the description of blockchain technologies to the minimum. Exhaustive reference books are Antonopoulos (2014) and DuPont (2019), or Drescher (2017).

argue that blockchain is developing as an organizational technology, i.e. defined by the entanglement between blockchain governance and use context. In fact, in order to certify authenticity without a formal organization as guarantor, all participants need to organize: they have to cooperate to keep the system as a whole running reliably in order to handle a finite number of authenticated records ('tokens' from now on[6]). In short, the capacity of authentication, defined by consensus algorithms and sealed continuously by miners, is relevant for governance purposes because it ties together software developers (or system designers, more broadly), miners (or whoever maintain the ledger), and users. No one of them can easily break away from the others without losing much more than they would by forking a FOSS project: developers without miners would see their tokens carrying no authenticity, thus value, and users would not follow suit. We chose records of used cars and land registries because they clearly illustrate these points.

After highlighting the constitutive organizational aspects of blockchains, this paper continues to identify the features of the mode of blockchain-related Hanseatic governance, which mediates between FOSS's fluidity and blockchains' immutability. Narrowing it down to an exploratory research question, our focus is on: How does blockchain governance differ from the governance of Free and Open Source Software (FOSS), often referred to as 'bazaar'? At this point it is important to note that in this paper we are focusing on designers and maintainers because their mutual dependency marks the major difference from FOSS.

The rest of the paper is organized according to the following argument line: like FOSS, blockchains spread beyond and outside of formal organizations but, unlike FOSS, use contexts constrain designers' freedom because of authenticity and immutability, without which there would be no reason for using a blockchain in the first place. So, blockchains differ from FOSS governance (data governance differs from tokens') because developers cannot do without partnerships with authenticators. These passages are first defined in their theorical relevance, then illustrated through contrastive empirical cases: The Decentralized Autonomous Organization's (The DAO from now on) governance problems demonstrate the failures of reducing governance to algorithms. Then, systems for second-hand car market and land registries show the role of consortia in mediating across diverse use organizations. Based on those cases, our conceptual answer to the research question is the metaphor of the Hanseatic League: an alternative, consortium-based governance model for organizational technologies.

Literature and Framework

Over the decades, governance has been defined in many ways. Williamson (1975) explains it as the explicit or implicit contractual framework within which a transaction is located, it pervades with order relations where potential conflict risks to hinder mutual gains. Even if transaction cost played a central role in influential studies on governance, it remains too narrowly focused on to economic explanations for our purposes. Beck et al. (2018) emphasize decision-making by understanding governance as the means for organizational and economic coordination utilizing decision rights, incentives, and accountabilities. According to Ziolkowski et al. (2019), governance describes how responsibilities and powers are aligned among actors, who decides, how the decision-making process is conducted, and how decision-makers are held accountable. In order to accommodate the diversity of use domains that blockchains are and can be applied to, here we consider relevant for governance as the ability to get actors to behave as they would not (adapted from Stoker (1998)). This relational definition of governance covers formal and informal power, thus different modes of organizing like markets, networks, hierarchies, or bazaar, and accounts also for powerful forces like prices, agreements, social norms, contingencies, hype, charisma, etc. which all proved explanatory in blockchain cases.

Since design and practice often differ substantially (Ciborra 2000), we searched for literature about blockchain, organization, and governance with a specific interest for blockchains in actual use, rather than for publications outlining the potentials of this emerging technology, e.g. Tapscott and Tapscott (2017) and Davidson et al. (2016), or Shermin (2017), who places her emphasis on reduction of transaction cost. Not least because of the long-time cycle of implementing IT, studying them, and going through peer-review processes, we could not find many academic studies of actually implemented blockchains used in real-life settings. So, this section starts with a few cornerstone studies from the emerging studies on blockchain, then it defines our broader framework starting with FOSS governance.

[6] Throughout this text, we use 'token' to refer to the items handled on both permissionless and permissioned blockchains.

Seebacher and Schüritz (2017) reviewed the literature on blockchain technology highlighting how it can enable services. Walsh et al. (2016) conducted a literature review to gain an overview of blockchain characteristics, a necessary step to define blockchain types: Decentralized/Extensible (Bitcoin), Decentralized/Inextensible (Counterparty), Centralized/Extensible (Ripple), and Centralized/Inextensible (R3). Beck et al. (2018) rely on the more established dichotomies permissioned/permissionless and public/private. The following table positions those dichotomies as general affordances for blockchain governance.

		Access to Transaction Validation	
		Permissionless	**Permissioned**
Access to Transactions	**Public**	All nodes can read, submit, and validate transactions	All nodes can read and submit transactions. Only authorized nodes can validate transactions
	Private	(Encrypted records can be pegged to permissionless blockchains for proof-of-existence)	Only authorized nodes can read, submit, and validate transactions

Table 1 Classification on Blockchain Types, modeled after Beck et al. (2018), based on Peters and Panayi (2015)

Beyond classifications like by Swan (2015), Morabito (2017) still offers the most exhaustive overview of the state-of-the-art of blockchains in organizations, especially in finance, supply chain management, health care. In all of them, the consensus mechanism is the centerpiece as it assures the integrity of the ledger and discriminates the validity of proposed transactions. These coordination mechanisms define how validators participate in the blockchain functioning. Scholz and Stein (2018) foreground the organizational aspect of blockchain and aim at showing specific novelties in comparison to other types of organizations. Digital immutability through native authentication, thus the possibility of governance through blockchains, is reflected in collaborative ventures to explore the benefits of blockchain technology both for profit and non-for-profit (Gratzke et al. 2017).

While permissioned blockchains can preserve some permissionless blockchain's characteristics such as decentralization, immutability, and auditability, they present a wider variety of features for identifying users, assigning transaction, validation, and access rights. Ledger maintenance here is rarely guaranteed by proof-of-work but by other, more efficient consensus algorithms like proof-of-stake or Byzantine fault tolerance among others (Zheng et al. 2017) (Mingxiao et al. 2017).

Given the lack of cases with a substantive role of end users, here we limit our focus on the governance 'of' blockchains. So, while we remain aware of the peculiarities of each domain of application and its end users, we do not expand in those directions here. Our theoretical framework is presented in two steps. First, the bazaar mode of governance – typical of FOSS – is introduced, then its explanatory limitations for blockchain are highlighted. Second, recent studies that help our theorization are discussed.

Organizing in the Open: the Bazaar

There are two related reasons why FOSS and its peculiar mode of governance is relevant when studying distributed ledgers of different sorts: blockchains software is more often than not released under FOSS licenses, and second, influential blockchain developers come from that environment, thus adopt and promulgate the same formal and informal rules, which emerged and consolidated on the open internet. The openness that the internet allowed has questioned and eroded the centrality of formal organizations in organizing societies, and originated numerous and sometimes influential concepts like the 'open innovation' (Chesbrough 2003), 'wisdom of the crowds' (Surowiecki 2005), 'the wealth of networks' (Benkler 2006), and 'generativity' (Zittrain 2006). Regarding the peculiar mode of online organizing, Raymond (1999a) first, and Demil and Lecocq (2006) later, labelled it 'bazaar' and relied on FOSS as the main illustration.[7]

[7] Regarding terminology, this article uses 'form of organization' and 'mode of governance' interchangeably. This is not only due to the literature of reference, which oscillates between the two terms (Demil and Lecocq 2006; Powell 1990), but also to our broad understanding of organizing, which underpins both. Following Czarniawska (2014), we understand organizing as a process that is broader than organizations, which are a relatively structured and stable way of organizing.

According to them, rather than formal hierarchical organizations – referred to as 'cathedrals' – online organizing resembles a bazaar, where individuals move in and out easily and organize on the basis of merit and reputation. David D. Clark, an early internet architect, captured this mode of governance with a slogan that became famous: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code." Remarkable successes of this mode of organizing, also referred to as 'commons-based peer production' (Benkler 2006), governed FOSS (Coleman 2012) and Wikipedia (Jemielniak 2014) (Aaltonen and Lanzara 2015).

The bazaar mode of governance emphasizes the non-appropriability of digital data, which originated as part of early software developers' practices of tinkering with code, subsequently became protected by open licenses. The effect is the obliteration of property rights, thus the impossibility of trading software. In the 90s these ideas and practices of free sharing of software were against all the received wisdom of product management, and the business model of software multinationals like Microsoft. Detractors claimed that without economic incentives to trade software, and hierarchies to manage its development, FOSS would fail. Instead, it thrived with an organizing mode that Raymond (1999a), who developed Fetchmail (a FOSS email client), likened to a 'bazaar' as opposed to the 'cathedral' of software corporations.

FOSS took a hegemonic position over the internet not only by ignoring much of the received wisdom about IT governance (Raymond 1999b), but also projecting the possibilities of open collaboration far beyond software development. For instance, Wikipedia has shown that peer production can be governed in such a way that it yields products superior to those produced by formal organizations like publishers (Jemielniak 2014). The FOSS literature has explored different aspects of this mode of organizing. Main foci have been: motivation and incentive – typically based on voluntary work and reputational benefits (Feller and Fitzgerald 2002) (Fitzgerald 2006), emphasis on the creativity that commons licenses allow (Benkler 2006), protection of the commons against overuse and vandalism (Benkler 2016). Notwithstanding its initial motives, over the years FOSS had to acknowledge that other forms of hierarchy emerged over time (Jemielniak 2014) (Shaikh and Henfridsson 2017). Something similar is happening to blockchains, although via a different path.

Following the more nuanced theorization of the bazaar by Demil and Lecocq (2006), developers build up their reputation, which in turn they can spend providing assistance on the software they know. So, the bazaar operates at an aggregated low level of control on actors' behaviors, not least because – having full access to source code – anyone can always fork their software and develop it in their own way. Since FOSS licenses are viral, forking reinforces the commons by spreading it rather than diminishing it. So, FOSS generates limited polarization of public vs. private compared to the long-lasting debate around the tragedy of the commons (Bollier and Helfrich 2014). The bazaar proved really effective and efficient in mobilizing dispersed resources. Nonetheless, its advantages become available only under specific conditions, not all met by blockchains. The issue is that the bazaar misses to account for the authentication that blockchain-related governance is characterized by (Miscione et al. 2018).

Bitcoin first, and other blockchains in subsequent years, have originated from the same bazaar mode of governance, which relies on public software repositories and globally distributed technical skills, privacy concerned actors, rejection of corporations and states (DuPont 2019) (Zheng et al. 2017). However, blockchains operate and develop differently from FOSS, especially because of the role of miners who maintain the blockchain by authenticating transactions in a way that also end users find satisfactory enough to trust the system. Their roles diminish software developers' freedom of taking the technology where they like. For these reasons, the bazaar does not explain the governance of blockchains. Since the ultimate test for an organizational technology lays in use organizations (which comprise authenticators and the variety of end users involved), and use organizations are constitutive of blockchains by authenticating the ledger they rely upon, then, emphasizing software design – like FOSS theorizations use to do – is misleading.

Bitcoin was the first blockchain that tested at scale a rewarding mechanism for keeping faceless and globally dispersed actors complying with its rules of authentication (Miscione et al. 2018). Differently from the abundance that operators in a bazaar take for granted, blockchain re-introduces scarcity and opens a prospect for a different governance. Blockchains are peculiar and interesting for governance because they promise to scale easily when they reach a critical mass, but they are difficult to manage because of lack of both formal organizational structures and clear boundaries to police (Ziolkowski et al. 2019).

In sum, blockchains originate from FOSS, but have profound differences. Bazaar governance is an open-ended organizational mode of software developers volunteering to code while remaining under low control and incentive pressures, thus building their skills and reputation. In contrast, blockchains as a matter of ex ante design, restrict the availability of tokens, enforce incentives, thus exercise a significant amount of control on all parties involved. In sum, tokens are governed differently from information goods and related bazaar governance (Raymond 1999a) (Demil and Lecocq 2006) because they embed organizational functions like consensus and authentication which define a remarkable level of mutual dependency among the parties involved. This main difference is made evident by forks, which delegitimize the authenticity of a distributed ledger, thus undermine the value of its tokens. Last but not least, tokens are not free because each has a production cost and transaction costs (its own's and of what it may stand for). Those differences motivate the need for formalizing our proposal for Hanseatic governance. To get there, this paper continues by first presenting contrastive case studies on the base of which our theorization is discussed later.

Authentication: open like the Internet and tight like Money

Against the background of the openness that the bazaar guarantees and depends upon, the major innovation introduced by blockchain – and proved viable at global scale by Bitcoin – is distributed authentication to avoid both double-spending and reliance on external guarantors. As a result, both blockchains' strengths and weaknesses depend on being, at the same time, open like the internet and tight like money. This anomalous combination of properties is certainly new and worth attention. Blockchains have been widely portrayed as trustless, which is usually interpreted as: blockchains are algorithmically governed, thus do not require interpersonal or institutional trust (Beck et al. 2016). However, they do require trust that the system has been properly designed and runs flawlessly, which also implies trust in the designers of the blockchain and in its maintainers. The DAO case exemplifies how this trust – like any trust – is precarious and may be unwarranted.

Lustig and Nardi (2015) investigate how Bitcoin's algorithm has gained authority and legitimation in allowing new trades. In this sense, algorithms are discussed as a way of directing human activities by defining what to rely upon. They criticize the emic views of people promoting Bitcoin for their naive assumptions about technological neutrality and independence from allegedly corrupted politics. A similar approach can be seen in the discussion on blockchain-based state governance (Atzori 2015) (MacDonald et al. 2016). Even if we agree that algorithms are not neutral in transforming human behaviors, organizations, and societies, we find that a narrow focus on algorithms does not account for novel aspects that blockchains bring to the fore when compared to the bazaar: authentication is guaranteed by miners and legitimized by users. These actors pass unseen by a narrow focus on algorithms. In practice, if we consider only algorithms, we would not see much difference between blockchain software code and blockchains in use, which depends on the authentication needs of specific domains. Distinctly from information technologies, the constitutive role of use organizations along software developers makes blockchain a relevant instance of organizational technologies because they automatize consensus and authentication within distinctive contexts of use, which are typical organizational functions.

Authentication is here intended in its basic meaning of certification of genuinity, i.e. each of the limited number of tokens in existence can be traced back to an owner at any point in time. This means that, although most blockchain software is open source (so it falls under the bazaar governance mode), tokens' authenticity (thus blockchains' value) depends on those who authenticate and use the ledger. The centrality of consensus maintenance sets blockchain design, development, and deployment apart from technologies that only compute and transmit information while leaving consensus and authentication to organizations. In short, governance cannot be conceived as an add-on topic but needs to be considered as constitutive of blockchain and its application domain.

This digital native way of authenticating tokens constitutes a qualitative shift from the abundance that defines the bazaar. Tokens moderate software design freedom to grant authenticity. For their users, this novel balance between openness and tightness allows for new arrangements. Nevertheless, Agre (2003) argues, we should not be deterministic about how technological architectures interplay with institutional arrangements. Use will tell how those interplays develop.

Methodological Notes

A useful analytical distinction is governance 'of' vs. 'by' blockchain. With the notable (but difficult to investigate) exception of illegal trades, blockchains have yet to prove the promised disruptions in organizations, sectors, industries, etc. So, the focus of our empirical work cannot be but on the governance 'of' blockchains. Governance 'by' blockchain, in which end users have a heavier weight, will be possible when more use cases will have run their courses. Because of space limitation, and since we have described our research methodologies in other publications, we refer to them (Miscione et al. 2018) (Ziolkowski et al. 2018) (Ziolkowski et al. 2019) (Kavanagh et al. 2019) for all details about those case studies.

When approaching any global information system like blockchains, especially Bitcoin and Ethereum (on which The DAO was based), methodological challenges arise. First, we considered Latour's suggestion to 'follow the actors'. As in many comparable cases, the main identifiable actors are the software developers. Focusing on them only would have been problematic because it would have implied an overemphasis on software design over use, which would overlook significant shortcomings of the explanatory power of the bazaar for blockchains. Second, other relevant actors might not be organized as visible communities with distinct values, venues of communication, and practices. So, Latour's recommendation presented substantial limitations not least because online actors using global blockchains can be millions, and key non-developer actors tend not to be easily identifiable nor visible. Then, we considered Czarniawska's recommendation to 'follow the actions'. This had the undoubted advantage of being agnostic about actors, but still did not solve the problem of sheer scale of the empirical domain. Thus, avoiding studying the more technical community simply because it was easier to identify and follow, left us with no specific actors to follow, and no specific actions to look at in the worldwide conglomerate of actions and transactions that define blockchains. The solution to this impasse presented itself.

In spite of the difficulties derived from the lack of clear boundaries defining who is who and what happens where (i.e. identifying and studying relevant actors, actions and places) it was clear from the fora and specialized press we had been following, that those involved in blockchains (especially permissionless) shared a sense of what constituted problems. Following Hoppe (2010), this situation suggested us to 'follow the problems' as they manifested and were dealt with. The general publicity of online organizing made the objective of following problems, and how they were dealt with by a multitude of actions, feasible.

Our focus on consortium-based blockchains is the result of long-term engagement in interorganizational systems. The two cases presented below are a large design science research project dedicated to improving the used car market, and an interview-based and documentary study of land registries. The consortium developing and deploying a distributed ledger for the second-hand car market was studied through participant observation in the frame of design research. While all authors are well-aware of the progress of this research project, two authors have prominent roles in it and have been documenting it extensively. Land registries have been investigated first through wide-ranging documentary analyses of online materials and gray literature provided by actors directly involved. Then, semi-structured interviews with key actors were conducted and when possible repeated over an extended period of time, so to grasp a sense of the evolution of those projects.

Illustrations of Governance 'of' Blockchains

The empirical section comprises three empirical cases: the first presents the exemplar governance crisis that affected The DAO, and the blockchain underneath it: Ethereum (the second largest after Bitcoin). Its rupture made its deeper functioning and risks visible. The following part presents two consortia-based blockchains, one for secondhand cars in Switzerland, the other for the land registry in Georgia. They present a viable alternative to the shortcomings of assuming the possibility of automatizing governance. All these case studies focus on organizational and governance issues and provide empirical evidence that blockchain is not conforming to the FOSS governance models. The DAO is representative of the governance shortcomings that permissionless blockchains manifested over the last decade. Thus, it is used as a theoretically informed steppingstone to introduce the crucial role consortia play in accommodating use organizations in the domains of secondhand car market and land registries. Those empirical findings are later discussed in the light of the metaphor to the Hanseatic League.

Loss of Innocence: no 'Complete Contracts'

The DAO was a social experiment in organizational governance. Its goal was to bring forth a decentralized and innovative business model, which would allow investors to transparently, democratically and fairly fund collectively voted projects using the raised cryptocurrency capital. Built upon Ethereum's smart contract feature, The DAO was the first of its kind. This spirit of openness and decentralization helped The DAO to gain traction quickly.[8] This visionary platform launched on April 30th, 2016. On May 28th, it raised approx. 14% of Ethereum's total currency supply and was the largest initial coin offering (ICO) by then. One bug in the code went unnoticed and was exploited on June 17th to drain about a third of the enclosed funds. However, a failsafe method allowed a voting period of 28 days before transactions are committed to the ledger. This timeframe allowed developers, users, and miners time to decide what measures to put in place. However, it quickly became apparent that this issue was out of The DAO's control. Its smart contracts had been executed accordingly to its design and credited to the idea of decentralization and 'code is law' principles, the contract contained no inbuilt measures to break ledger's immutability to expropriate the attacker. As a matter of facts, the attacker complied with the smart contract's rules and thereby, some argued, obtained the funds technically correct, thus legally. As a result, The DAO's incident could only be solved on the underlying layer, i.e. Ethereum blockchain. The project's prominence henceforth put financial, media, and legal pressure on Ethereum's community to make an appearance and decide on the event's handling.

Following this exploit, a group of The DAO's and Ethereum's lead developers and community members teamed up quickly and convinced major exchanges to halt the native Ethereum's token trading, which was the currency of the stolen capital. Simultaneously, white-hat counter attacks drained and secured the remaining funds, which by the community was perceived as taking the 'role of fiduciary to The DAO and its members'. Having averted further and imminent threats, the loathed politics that cyber-libertarians aimed at eradicating with decentralized blockchains retook front and center stage. Despite the confusion arising from not having roles for who is in charge of what, the options boiled down to either ignoring and accepting the exploit, or introducing changes to Ethereum's protocol, i.e., forking. Two opposing factions emerged in this debate, one called for an amendment, i.e. a hard-fork, and one that opposed any interference. Supporters of the latter persuasion argued that 'transactions are immutable and code is law'.[9] Unlike in a bazaar setting, a hack of the ledger to reverse the exploit would contradict both core beliefs and purpose of decentralized authentication. Members of this sentiment considered any intervention a 'centralized bailout [of a] decentralized protocol'[10] and described The DAO as being 'too big to fail'[11]. By contrast, forking advocates regarded the proposed amendment to depict 'business as usual'[12], claiming[13] that fixing bugs within protocols has always been part of software development processes. By arguing so, the latter framed the interpretation according to the bazaar mode of production and away from the authenticity and immutability aspect that blockchains are rooted in.

Ultimately, miners, not developers, decided on the outcome by committing their hash power to the favored chain. The faction opposing the fork eventually turned out to be in the minority and blamed, among others, Ethereum's founder, Vitalik Buterin, for exerting his political clout in favor of breaching technical immutability through human intervention. The presence of Ethereum's 'benevolent autocrat' became well visible in this situation, distinguishing it from Bitcoin and its anonymous founder who withdrew completely and appeared no more during debates to voice his well-respected opinion, letting factions flying the flag of his writings. One user voiced his view on the situation by concluding 'chancellor Vitalik on brink of first bailout for DAOs'.[14] Some miners and users refused to acknowledge the new protocol and continued to apply the original ruleset. This inevitably caused the fork and induced a chain-split, dividing the project into two distinct blockchains. While the original blockchain is since referred to as 'Ethereum Classic', the current Ethereum main chain is actually the forked one, not the original. Following this precedent and its evident

[8] https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5
[9] https://www.reddit.com/r/ethereum/comments/4unpm3/the_dao_and_the_benefactors/
[10] https://www.reddit.com/r/ethtrader/comments/4oif5c/fck_this_dao/
[11] https://www.reddit.com/r/ethereum/comments/4oithy/a_too_big_to_fail_political_hard_fork_is_very/
[12] https://www.reddit.com/r/ethereum/comments/4op69x/no_hard_fork_does_not_mean_dao_holders_lose_all/
[13] https://www.parity.io/attack-on-the-dao-what-will-be-your-response/
[14] https://btc.com/86f03176beef99ac2f5adecd39b964f874f5ec615a9d01e88ac781c6e669753c It is worth noting here that cryptocurrency advocates matured a deep resentment for bailouts and quantitative easing policies by 'central authorities'.

consensus-making complications, one user aptly wondered 'if there will ever be a consent on proposals with that many shareholders'.[15]

Altogether, a single project's failure became a broader community's concern, forcing it into internal disputes and re-interpreting its core values: as no compromise solution was available, any decision would either lead to infringing Ethereum's immutability and thereby betraying decentralization's and its fundamental values, or losing valuation and the user's assets. One part regarded the outcome a 'legitimate community response'[16], the other saw the tyranny of the majority in the voted solution the '[ending] of what Ethereum was always meant to be'[17]. However, most of the fork opposers ultimately applied the new ruleset, understanding Ethereum to be a 'democracy, not technocracy'[18] in which 'all that matters is consensus'[19], even if executed algorithmically.

For the sake of the present argument, The DAO case illustrates three points:

- contracts are not and cannot be complete – thus their assimilation to software code, which always contains bugs, is hazardous – and always depend on the wider context they operate in,
- there is – by definition – no response to unforeseen shortcomings of the code, which exposes the risks and the required trust into the system, its designers and its maintainers,
- if immutability is only alleged, derived claims of substituting governance with blockchains become questionable.

The other cases and the following discussion discard the dichotomy governance vs. blockchain, and argue that blockchains are indeed organizational technologies with a peculiar mode of governance through consortia that retain some of the powers that permissionless blockchains tried to delegate completely to technology. These consortia-based blockchains aim at avoiding governance problems exemplified by The DAO by creating an – albeit imperfect – governance structure with case-specific tailoring of access and authentication rights, allocation of responsibilities, reliance on existing jurisdictions and institutional contexts (Ziolkowski et al. 2019).

Tackling Information Asymmetry in the Second-hand Car Market

This case illustrates a consortium-based blockchain to deal with the used car market, where good and bad cars are not easy to distinguish, thus: a) parties with better information are more likely to strike better deals, and b) worse cars drive better ones out of the market (Akerlof 1970). The ability to make a good assessment of a car's value relates to the completeness and reliability of information about it. However, obtaining relevant car information can be a daunting endeavor. In other terms, information asymmetry is inherent to the used-car market. This project's developers were early on interested in how far a distributed ledger may reduce information asymmetry between buyers and sellers, thus reducing the negative influence of 'lemons' onto the used car market. Consequently, they adopted an information management angle rather than an economic one. In other words: a complete record of information combined with traceability and authenticity of information, which blockchain provides natively, may reduce the current asymmetry of information.

During the lifetime of a car, numerous actors (insurances, repair shops, state agencies, and many more) are involved. This leaves all information about a car fragmented at best, or even exposed to opportunistic behaviors. In practice, it became apparent that creating a more consistent and reliable record of cars (AutoFile from now on) requires the coordinated effort of many actors. Therefore, the developers proposed a blockchain-based platform, which would act as a boundary object mediating across stakeholders to overcome the shortcomings of a market for lemons.[20]

The AutoFile is run by a consortium of major stakeholders in the Swiss automotive market: The AutoFile consortium comprises organizations at all points of the value chain, as well as competitors: The main importer and repair shop of cars, a major insurance company, a road traffic authority, a car rental provider.

---

[15] https://www.reddit.com/r/ethereum/comments/4ihkld/the_dao_must_diversify/
[16] https://www.parity.io/attack-on-the-dao-what-will-be-your-response/
[17] https://www.reddit.com/r/ethereum/comments/4oj7ql/personal_statement_regarding_the_fork/
[18] https://www.reddit.com/r/Futurology/comments/2bypb7/does_an_automated_society_still_need_humanrun/
[19] https://www.reddit.com/r/Bitcoin/comments/2fch1l/would_you_argue_that_bitcoin_has_more_or_less/
[20] It is worth noting that there are two problems about those records: their completeness and their integrity. A blockchain can address only the second.

The actual development was driven by a software company, researchers, and legal experts. One major challenge has been the coordination of interests and governance mechanisms. When the development reached a maturity where a launch of the platform was foreseeable, the consortium founded a non-profit association to provide a point of reference for governance of the shared platform. This effort was also motivated by the need (1) to onboard the critical mass of users the platform rests upon, and (2) the ability to prototype business processes in a real-life setting, (3) to provide a meeting place where also the state agencies could participate. The last point has a particular governance relevance: while a good used-car market is of public interest (which lemons' sellers skew), it is difficult if not impossible to manage the AutoFile as a public good. Therefore, an association offers the chance for a public-private partnership to negotiate both public and private interests through the design and deployment of novel services.

This consortium agreed on an association's statute comprising core rules such as membership rights and obligations, the association's purpose, fee structures, and thereby serves as a playbook for a novel ledger before it is finalized and sealed as immutable by authenticators. If conflicts emerge in the future, standard societal and legal modes of conflict resolution would apply. One may object that this choice limits innovation potential, but participants decided to build on the existing institutional context, which is conceived as an enabler rather than an obstacle to innovation. For instance, a cantonal traffic authority joined to instill credibility into the project since its inception.

The entanglement between blockchain governance and institutional context is particularly evident in relation to the legal framework regulating privacy, which emerged as a defining issue early in the process. Personal and car-related data cannot be distinguished easily from each other. While the sharing of the latter is generally harmless, the former is quite sensitive, and heavily regulated, especially by the GDPR. Since drawing the line between the two is all but straightforward, the system had to be designed to compartmentalize different kinds of data and keeping each tied to their legally bound organization. Because of this, a first proof-of-concept built on Hyperledger had to be abandoned. In fact, distributing all data across all participating nodes, even if encrypted, proved not fit for the project's purposes. If all data is shared across all nodes, the association would have no mean to terminate local data usage because every participant would manage a full node independently.[21] Therefore, the AutoFile consortium moved in the opposite direction of delegating as much as possible to technology. It adopted a distributed ledger because of its higher flexibility and governance discretionality it leaves to the association.

Privacy issues can be seen as exemplar of how distributed authentication interplays with data ownership, usually marginally considered in bazaar settings, and multiple lines of responsibility. Regarding the latter, even if the association comprises multiple organizations, there is not a hierarchical level above them. Each organization upholds responsibility on the data it brings to the ledger. For instance, an insurance company may share (part of) their clients' data (like about accidents) on the shared ledger, but it remains responsible for them in front of its clients and legal authorities. Issues like this illustrate the organizational complications that such consortia have to deal with, and the risks of delegating as much as possible to automated governance before having used the blockchain in a real-life setting. The other blockchain governance issue is the mutual dependency between developers and maintainers. Since it is clear to all parties that forking would undermine the validity of the ledger, association members are required partnership fees to join. This is because having 'skin in the game' reduces the risks of opportunistic behaviors later on.

Certifying Land Ownership beyond Jurisdictions

Even if the AutoFile sees the participation of a public traffic authority to the consortium, state organizations are not as central as in other sectors like urban and regional planning, and land management more precisely. The land registry domain is a promising use case for blockchain as noted at the World Economic Forum (Hutt 2016). Blockchain-based land registries come with the promise of overcoming several of the challenges of this complex and multi-stakeholder inter-organizational setting (landowners, brokers, notaries, banks, and state agencies) with far-reaching ramifications in all parts of economy and society. The processes of authenticating land ownership and transfer vary vastly between jurisdictions, but several com-

[21] Incidentally, similar kind of concerns about potential uses are affecting the Libra consortium and its negotiations with regulators, who expressed their concerns about how to comply with KYC (know your customers) and AML (anti-money laundry) duties in a cross-jurisdictional setting.

monalities are observed: they can be considered slow, sparsely digitized, often opaque, costly, and embedded into very low trust environments. Because of its high valuations at stake, not least for its use as collateral, land registration is heavily exposed to fraudulent behaviors which have been particularly problematic in developing countries (De' 2005; De' and Sen 2004) (Benbunan-Fich and Castellanos 2018).

Immutability of blockchain records have a particular significance in places prone to corruption, fraud, natural catastrophes, political instability, or, in extreme cases, invasions. Fraudulent renting, expropriations, extortion, and bribery in dealing with governmental or notary third parties are not uncommon (Ziolkowski et al. 2018). This is not to say that blockchains would overcome all these challenges, but they might ease these problems and increase the reliability of records by offering a tamper-resistant, decentralized database[22]. We have been surveying projects and consortia dedicated to blockchain-based land registries in many countries, including Sweden, Estonia, Honduras, Ghana. Here we focus on Georgia for the peculiarities of this case.

"The economist Hernando de Soto told us that only one third of all people can prove they own their land. Apart from the legal uncertainty, there is $20 trillion in dead capital, as land with unexplained legal titles cannot be sold. So, we told him, 'Find us such a country and we bring the land register to the Blockchain for free. And that was Georgia"[23] stated a member of this consortium. Associated actors, such as banks, notaries, and Georgia's National Agency of Public Registry (NAPR) are loosely coupled and cannot trace processes amongst each other, mistakes occur, and they are costly to correct, also for citizens. Furthermore, all NAPR servers are centralized. Hence data can relatively easily be tampered with or even destroyed, for example in the extreme case of an invasion, which is less remotely possible than for other countries: the last war with Russia dates merely ten years back; less than four years ago, Russia annexed Crimea, which is only across the Black Sea from Georgia. NAPR employees have mentioned all of these as motivation in their effort to build a blockchain-based land registry which is also pegged onto the Bitcoin blockchain, thus beyond the reach of any occupying force.[24]

While in developed economies efficiency is often a selling factor for blockchains, in Georgia security concerns score far more prominently. In fact, immutability and extra-jurisdictional reach of blockchains is seen a potential succor against a threatening neighbor. The risk NAPR is trying to avoid is not only that occupying forces destroy ownership records and appropriate land. It is not unthinkable that records can be wiped out through a cyberattack, which has become a common concern in former Soviet countries like Ukraine.[25] This is an illustrative example of how governance of blockchain (editing access to land records, for example) exceeds a national legal framework and addresses broader concerns through a mix of cryptographic authentication run by Bitcoin miners without any specific interest for this countries, but whose activities are beyond the reach of a state power. Leaving aside those extreme circumstances, pegging land records to the Bitcoin blockchain in the form of a hash at specified points in time through a digital time-stamping service[26] offers a proof-of-existence and serves as a checkpoint to prevent also smaller scale fraudulent tampering of past transactions.

Another central issue, which too often is conflated with immutability, is how to certify data quality before it gets on an immutable ledger. In Georgia, the NAPR is responsible for data entry to the system, which requires trust in its reliability (Ziolkowski et al. 2018). However, NAPR foresees an important measure to increase transparency: it is allowing other parties (banks, notaries, NGOs, and later also citizens) to read the ledger, which contains all historical data, and thereby to control the well-functioning of the system.

---

[22] Reese, F. 2017. "Land Registry: A Big Blockchain Use Case Explored," CoinDesk, , April 19. (https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem, accessed November 26, 2018)

[23] https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c

[24] The system is called 'Exonum', an explanation how it specifically works can be found here: https://exonum.com/napr

[25] Also documented here: https://www.newamerica.org/future-property-rights/blog/blockchain-for-property-rights-georgia/ and https://www.reuters.com/article/us-estonia-cybersecurity/with-an-eye-on-russia-estonia-seeks-security-in-computing-cloud-idUSKBN0TN1BT20151204

[26] Shin, L. 2016. "Republic of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury," Forbes, April 21. (http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/, accessed May 18, 2017).

Hanseatic Governance

Our research question was: 'How does blockchain governance differ from the governance of Free and Open Source Software (FOSS), often referred to as 'bazaar'?' The internet opened up for a very effective mode of governance which relies upon non-scarcity of data: the bazaar, of which FOSS and Wikipedia successes are glaring examples. The bazaar mode of governance relies upon licenses that protect the nearly zero marginal cost of reproduction and distribution of data. Against this background, our research problem has been that the bazaar does not explain essential peculiarities of blockchain governance. More precisely, blockchain originated from the need of avoiding 'double-spending', i.e. duplication of data, without putting any formal organization in charge of authentication. Blockchains escape main tenets of the bazaar mode of governance because maintainers remain in charge of authentication. Thus, designers are tied to them to certify and extend the value of the blockchain. In other words, the bazaar's emphasis on software production overlooks use and the inter-organizational mutual dependency of all parties. Guaranteeing the immutability of all records on a ledger generates a much tighter path dependency than in the bazaar. Software developers may be free to fork the code, but it is of little use in practice if parties cannot trust records about used cars or land parcels, following the examples above. Therefore, we argue that maintainers and users of tokens characterize the governance issues of blockchains. Authenticity is not a straight product of algorithms but a sustained long-term effort that all involved parties contribute to and depend upon. Beyond software developers, miners (or whoever maintains the ledger), generators of reliable records, and uses have to be included in any governance model. More precisely:

1. While in the bazaar the majority cannot enforce its decisions onto everyone, because anyone can fork their own version relying on publicly available code at low cost while preserving their own use value, in blockchain matters majority decisions are enforced, and forking poses substantial problems to both developers and maintainers;
2. Contrary to open source licenses that prevent anyone from appropriating the software code, public ledgers introduce authentication thus scarcity into digital settings. Traceability of all (trans)actions on the ledger act as a deterrent from breaking the rules. So, blockchain move from 'carrots and rainbows' as main incentives (von Krogh et al. 2012), to a 'gentle rivalry' within a consortium like the AutoFile (Ziolkowski et al. 2019);
3. The uncertainty about tomorrow puts more pressure on what is done today because forking later on would be troublesome. Consortium-based projects do not assume the possibility of future-proof complete contracts but rely on existing legal arrangements according to which all partners are tied together by mutual dependency.

Throughout this paper, we have emphasized how the peculiarities of using blockchains are in mutual dependency with their design. Our proposition is that this is a peculiar governance model, which is going to interplay with a variety of application domains. Before characterizing it as Hanseatic governance, we use a table to contrast and compare blockchain governance characteristics with FOSS and proprietary software.

All examples in Table 2 deal with goods that need varying degrees and modes of protection for different reasons. Counterfeiting is a key issue for proprietary software and the blockchains examples. Uncontrolled access is an issue when property of information goods (proprietary software) or privacy of people (financial assets) are a concern. For cars and parcels, certification of records is paramount, controlling access may be a matter of policy (who has the right to access and for what) or a commercial issue (monetizing information access). The three blockchain examples deal with very diverse institutional pressures. What connects them is the defining role of immutability and authenticity, which originates mutual dependency among the parties involved. The consequences of these peculiar arrangements are about balancing cooperation and competition while avoiding forking, and thus undermining blockchain authenticity. Those same problems and rationales manifested also in The DAO example, and its underneath blockchain Ethereum. They shape any blockchain that promises unique tokens standing for something else (AutoFiles, land registries, health records, goods tracking, etc.), data quality (accuracy of the ledger), unique relation between an object and its record, liability.

		Proprietary Software	FOSS	Bitcoin/The DAO	AutoFile	Land registry
Scarcity and protection of the matter of trade	Product protection	Legal: Transnational enforceable copyright Technical: DRM copy protection, license management	Legal: Licensing agreement for reuse (GNU, CC)	No legal protection Technical: Cryptographic consensus mechanisms to authenticate transaction. Forking as option of last resort	Existing national and international legal framework, especially GDPR Technical: cryptographic consensus mechanisms to authenticate transactions	Existing national legal framework Technical: Cryptographic consensus mechanisms to authenticate registry entry (and updates)
	Production input	Hierarchy with paid software developers	Bazaar of volunteer developers, reviewers, quality managers	Bazaar of volunteer developers, reviewers, quality managers Miners who get rewarded with the tokens they authenticate	All parties join up in a consortium that agrees with designers of the organizational set-up Developers and maintainers are part of the consortium	Digitization of existing records Pegging them to an extra-jurisdictional blockchain Planned: introduction of smart contracts
	Revenue model	Licenses to users and hardware vendors	Primary: None Secondary: Value added services	Transaction fees Hoarding	Partnership fees Planned: information access charge	Possible cost recovery models: taxes and/or fees
Organizing aspects	Means of regulation	Software platform monetized through license fees & sales	Peer produced software protected by copyleft licenses	Peer produced tokens	Consortium agreeing on what to make immutable, thus delegate to maintainers, and what to keep discretionary	Consortium built around the state land registration authority
	Path dependency	Investments of software industry and users	Collaborative practices for versioning, compatibility	Immutability ➔ Versioning via majority consensus or forking	Immutability ➔ Versioning via association deliberations	Immutability ➔ Versioning via consortium deliberations (state veto power)
	Overall governance	Hierarchy (ownership)	Community, meritocracy of production, agnostic about use	Minimal, derived from FOSS, rules, roles and incentives defined ex ante	Defined by use organizations in association. Records sealed by blockchain	Defined by use organizations lead by NAPR. Records sealed by blockchain
	Conflict resolution	Hierarchy	Community, forking	Majority rules	Car Dossier association (statutes) Existing legal frameworks	Existing legal frameworks Extra-jurisdictional blockchain as last resort

Table 2. Characteristics of exemplar cases against governance dimensions

Blockchain consortia are defined by people, organizations, and their environments more than endogenous incentive schemes on permissionless blockchains. The – loathed by crypto-libertarians – politics of creating alliances are central to define consortia's discretionary powers, which, coupled with the reliance on the existing institutional context, allow them to cope with the inevitable unpredictability of future situations. Thus, we name this mode of governance 'Hanseatic' after the Hanseatic League of the 13th to 16th century, after the fragmentation of feudalism and before the consolidation of modern nation-states in Europe, whose Rule of Law's subsequent rise to powers marked the League's decline. With the Hanseatic League, trade guilds across many cities spanning from nowadays Holland to the Baltic countries formed alliances that proved hegemonic in Northern Europe trade through the North and the Baltic Seas. The Hanseatic League's favor for orderly trade over conflicts resulted in a protracted period of prosperity and peace. It is suitable to underline that this alliance leveraged resemblances and common interests between member cities while marking their difference from the rest, but without undermining their independence.

The Hanseatic League used to have its own mode of governance, which was heavily relying on trust rather than defined by an overall constitutional framework like the Rule of Law of modern states. Another reason to adopt this metaphor is the role of the guilds, professional associations that influenced the League's decisions, similarly to expert organizations having a more prominent role in consortium-based blockchains (in the AutoFile: university, software company, traffic authority, lawyers, etc.). The Hanseatic League also provided aids for safe navigation (including lighthouses and safe harbors), and defended its members from the constant threats of pirates. For reasons of space, the following table illustrates how aspects of the Hanseatic League correspond to blockchain governance by relying on the AutoFile case, only.

	Hanseatic League	**AutoFile**
Share-holders	Coalition of German towns and merchant communities (horizontal alliance [or more loosely coalition] to compete successfully with other alliances or individual actors)	Coalition of stakeholders interested to build secondhand car records and at the same time avoid any kind of monopoly
Objective	Protecting mutual trading interests: Trade facilitation, mutual protection, trade monopoly in a region (not of any member over the others)	Interested in higher transparency in the used car market and committed towards basic governance principles: public service for Switzerland, non-monopolistic access charge. Second phase: data markets
Mode of operation	• Reciprocity, economies and politics of scale • "inside maneuver: extending competence/ resource base" • "outside maneuver: extending control over the environment" • Risk sharing • Mechanisms of (self-)protection	Joint (collective) production and governance of car lifecycle information infrastructure
Pitfalls	Obstacles to trade: • Logistics, reciprocal exchanges – economic challenges • taxation, customs, levies – legal, but costly (financially and process-wise) • piracy – illegal, requires protection ("libertarian" logic: we have to rely on ourselves).	Risk of monopolization or fragmentation of "market" for used car information. Need to ensure: • information quality, • certification/ authentication of information (or relevant access token), • Protection against unintended exploitation of the infrastructure.
Shared assets technology	"The four Kontore at London, Brugge, Bergen, and Novgorod were communities that enjoyed exemption from the jurisdiction of the land in which they were established, administering their own (German) law and subject to the directives of the Hanseatic diet." Encyclopedia Britannica Design of a boat type (Baltic cog).	Agreement on technical standard (blockchain/ crypto algorithms) and common (production and access) infrastructure.

Table 3. Matching of aspects of the Hanseatic League and our main blockchain case, the AutoFile

The resonance between the Hanseatic League and a blockchain motivates to propose the peculiarities of Hanseatic governance as different from the bazaar, defined by resource abundance and organizational fluidity. It is noteworthy that we do not claim that this mode of governance is an ideal type like hierarchy, market, or network ('confederation' might be). Rather, we define it as a lens to look at governance of blockchains. Following from Table 3, we characterize Hanseatic governance as follows:

1. Creating a framework for collaboration based on an agreed set of goals and incentives.
2. Setting-up an institutional and technical infrastructure (including traceability and reliability of the records) exceeding specific organizational domains or jurisdictions to increase effectiveness of operations and joint protection against perpetrators,
3. partial[27] delegation of typical organizational functions like consensus and authentication to technology (Hanseatic trade was made safer by specific boats and lighthouses, for example),

[27] This partiality is indirectly corroborated by the fact that no other technology is so closely tied to jurisdictions, especially small and agile ones like Switzerland, Malta, Liechtenstein, Gibraltar.

4. need to anticipate and negotiate early in the consortium the known, and possibly unknown, scenarios ahead of the initiative (similarly, Hanseatic allies had to organize for the long journeys of their cogs), and agree on what automatize and what keep discretionary.

Blockchains as Organizational Technologies

In terms of theoretical contributions, this work claims, on one side, that existing governance conceptualizations do not explain distinctive characteristics of blockchain, and that Hanseatic governance has a better explanatory power. On the other side, that blockchains can be seen as an instance of 'organizational technologies', by which we mean technologies whose core function is not transmitting information, but perform functions – inevitably entangled in and sensitive to an institutional context – that use to pertain to organizations, like consensus and authentication.

Despite their accomplishments, blockchains showed the limitations of rejecting explicit, and more sophisticated, modes of governance. Glaring failures have been efforts to change the Bitcoin block size and The DAO. The empirical issue with theoretical relevance is that the openness of the bazaar, which enacts a mode of software production, clashed with the immutability of those ledgers and their dependence on use organizations. These mismatching logics are evident in cases of forking: from a bazaar perspective it is a manifestation of freedom, if not simply 'business as usual', whereas for blockchains forks undermine uniqueness and immutability of tokens. Thus, blockchain mode of governance is distinctive, and we likened it to the Hanseatic League for the prominence given to mutual dependability within an alliance and the extraordinary organizational achievement to build a trade network and indeed infrastructure, which lasted well over 200 years. Application domains like second-hand car market and land registries showed how this technology is providing organizational functions that redefine organizational behaviors.

Authentication used not to be a function of FOSS projects, nor of digital-only endeavors. The novelty of blockchains is not in how they were peer produced, which resembles most FOSS projects, but in the authentication they allow in partnership with authenticators, that remove the fluidity and open creativity of the bazaar. Benkler (2016) classified different forms of digital collaboration like crowdsourcing, online labor markets, prize competitions, peer production depending on their complexity and knowledge. According to his view, open innovation produced by firms organized in networks lies in-between highly decentralized and innovative peer production and routine and predictable crowdsourcing. In his analytical scheme, blockchain-based governance is not a point on a chart, but a governance arrangement which might facilitate the growth of 'networks of firms' both in the direction of peer production (online actors can rely on tokens to formalize their transactions) and, on the opposite direction, towards online markets and crowdsourcing to the extend immutable ledgers increase security and may reduce transaction costs.

In conclusion IT has been changing how things get organized for decades now. Peer-to-peer networks, cloud computing, social media, to name just a few waves of digital innovation, are instances of a mode of organizing which has been: a) circumventing the structures and conventions of formal organizations, and b) changing and disrupting markets while opening new ones. The most recent trend of digital innovation is blockchain, which embeds functions that used to be the domain of organizations: consensus and authentication. In a nutshell, the contribution of this paper is that Hanseatic Governance accounts for the necessary mediation between the openness of the bazaar and the immutability of distributed ledgers. Consortia retain some powers to reach consensus when inflexible, preset algorithms cannot. Long-term consequences in governance remain largely to be studied in practice, especially where other forms of authority cannot be taken for granted. In prospect, reliable records embedded in an organizational infrastructure are promising in low trust environments, like where states or other authorities are weak. The modes of those encounters would offer promising research avenues.

References

Aaltonen, A., and Lanzara, G. F. 2015. "Building Governance Capability in Online Social Production: Insights from Wikipedia," *Organization Studies* (36:12), pp. 1649-1673.

Agre, P. E. 2003. "P2P and the Promise of Internet Equality," *Communications of the ACM* (46:2), pp. 39-42.

Akerlof, G. A. 1970. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism" *The Quarterly Journal of Economics* (84:3), pp. 488-500.

Antonopoulos, A. M. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies,* Sebastopol, CA: O'Reilly Media.

Atzori, M. 2015. "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," available at: http://dx.doi.org/10.2139/ssrn.2709713.

Beck, R., Müller-Bloch, C., and King, J. L. 2018. "Governance in the Blockchain Economy: A Framework and Research Agenda," *Journal of the Association for Information Systems* (19:10), pp. 1020-1034.

Beck, R., Stenum Czepluch, J., Lollike, N., and Malone, S. 2016. "Blockchain–the Gateway to Trust-Free Cryptographic Transactions," *available at: https://aisel.aisnet.org/ecis2016_rp/153*

Benbunan-Fich, R., and Castellanos, A. 2018. "Digitization of Land Records: From Paper to Blockchain," *available at: https://aisel.aisnet.org/icis2018/ebusiness/Presentations/15/*.

Benkler, Y. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom,* New Haven, CT, London: Yale University Press.

Benkler, Y. 2016. "*Peer Production and Cooperation*," in *Handbook on the Economics of the Internet,* J. M. Bauer & M. Latzer (eds.), Cheltenham and Northampton: Edward Elgar Publishing, pp. 91–119.

Bollier, D., and Helfrich, S. (eds) 2014. *The Wealth of the Commons: A World Beyond Market and State.* Amherst, MA: Levellers Press.

Chesbrough, H. W. 2003. *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Boston, MA: Harvard Business School Press.

Ciborra, C. U., Braa, K., Cordella, A., Dahlbom, B., Failla, A., and Hanseth, O. 2000. *From Control to Drift: The Dynamics of Corporate Information Infastructures*. New York, NY: Oxford University Press.

Coleman, E. G. 2012. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Czarniawska, B. 2014. *A Theory of Organizing*. Cheltenham: Edward Elgar Publishing.

Davidson, S., De Filippi, P., and Potts, J. 2016. "Economics of Blockchain," *available at http://dx.doi.org/10.2139/ssrn.2744751*.

De', R. 2005. "E-Government Systems in Developing Countries: Stakeholders and Conflict," in *Electronic Government. EGOV 2005.* Wimmer M.A., Traunmüller R., Grönlund Å., and Andersen K.V. (eds), Berlin, Heidelberg: Springer, pp. 26-37.

De', R., and Sen, C. 2004. "The Complex Nature of E-Government Projects: A Case Study of Bhoomi, an Initiative in Karnataka, India," in *Electronic Government. EGOV 2004.* Traunmüller R. (ed.), Berlin, Heidelberg: Springer, pp. 556-557.

Demil, B., and Lecocq, X. 2006. "Neither Market nor Hierarchy nor Network: The Emergence of Bazaar Governance," *Organization studies* (27:10), pp. 1447-1466.

Drescher, D. 2017. *Blockchain Basics: A Non-Technical Introduction in 25 Steps. Blockchain Basics: A Non-Technical Introduction in 25 Steps,* New York, NY: Apress.

DuPont, Q. 2019. *Cryptocurrencies and Blockchains*. Weinheim: Wiley-VCH.

Feller, J., and Fitzgerald, B. 2002. *Understanding Open Source Software Development*, London, Addison-Wesley.

Fitzgerald, B. 2006. "The Transformation of Open Source Software," *MIS Quarterly* (30:3), pp. 587-598.

Gratzke, P., Schatsky, D., and Piscini, E. 2017. "Banding Together for Blockchain,." *Deloitte Insights*, available at https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/emergence-of-blockchain-consortia.html

Hoppe, R. A. 2010. *The Governance of Problems: Puzzling, Powering, Participation*. Bristol, Policy Press.

Hutt, R. 2016. "Beyond Bitcoin: 4 Surprising Uses for Blockchain," *available at https://www.weforum.org/agenda/2016/12/fighting-human-trafficking-tracing-blood-diamonds-and-other-surprising-uses-for-blockchain/*.

Jemielniak, D. 2014. *Common Knowledge?: An Ethnography of Wikipedia*, Stanford, CA, Stanford University Press.

Kavanagh, D., Miscione, G., and Ennis, P. J. 2019. "The Bitcoin Game: Ethno-Resonance as Method," *Organization* (26:4), pp. 517-536.

Lustig, C., and Nardi, B. 2015. "Algorithmic Authority: The Case of Bitcoin," in *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS),* IEEE, pp. 743-752.

MacDonald, T. J., Allen, D. W., and Potts, J. 2016. "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking," in *Banking Beyond Banks and Money*, Tasca P., Aste T., Pelizzon L., Perony N. (eds.), Cham: Springer, pp. 279-296.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., and Qijun, C. 2017. "A Review on Consensus Algorithm of Blockchain," in *Proceeding of the International Conference on Systems, Man, and Cybernetics (SMC)*: IEEE, pp. 2567-2572.

Miscione, G., Ziolkowski, R., Zavolokina, L., and Schwabe, G. 2018. "Tribal Governance: The Business of Blockchain Authentication," in *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS),* IEEE.

Morabito, V. 2017. "Business Innovation through Blockchain," Cham: Springer.

Peters, G. W., and Panayi, E. 2015. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," *SSRN Electronic Journal arXiv:1511.05740*.

Powell, W. 1990. "Neither Market nor Hierarchy: Network Forms of Organization," *Research in Organizational Behavior* (12), pp. 295-336.

Raymond, E. S. 1999a. "The Cathedral and the Bazaar," *Knowledge, Technology & Policy* (12:3), pp. 23-49.

Raymond, E. S. 1999b. *The Cathedral and the Bazaar*. Sebastopol, CA: O'Reilly Media.

Scholz, T., and Stein, V. 2018. "The Architecture of Blockchain Organization," available at *https://aisel.aisnet.org/icis2018/crypto/Presentations/1/*.

Seebacher, S., and Schüritz, R. 2017. "Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review," in *Proceedings of the International Conference on Exploring Services Scienc*e (LNBIP, volume 279), Cham: Springer, pp. 12-23.

Shaikh, M., and Henfridsson, O. 2017. "Governing Open Source Software through Coordination Processes," *Information and Organization* (27:2), pp. 116-135.

Shermin, V. 2017. "Disrupting Governance with Blockchains and Smart Contracts," *Strategic Change* (26:5), pp. 499-509.

Stoker, G. 1998. "Governance as Theory: Five Propositions," *International Social Science Journal*, (50:155), pp. 17-28.

Surowiecki, J. 2005. *The Wisdom of the Crowds*, New York, NY: Anchor.

Swan, M. 2015. *Blockchain: Blueprint for a New Economy*, Sebastopol, CA: O'Reilly Media.

Tapscott, D., and Tapscott, A. 2017. "How Blockchain Will Change Organizations," *MIT Sloan Management Review* (58:2), p. 10.

von Krogh, G., Haefliger, S., Spaeth, S., and Wallin, M. W. 2012. "Carrots and Rainbows: Motivation and Social Practice in Open Source Software Development," *MIS Quarterly* (36:2), p. 649-676.

Walsh, C., OReilly, P., Gleasure, R., Feller, J., Li, S., and Cristoforo, J. 2016. "New Kid on the Block: A Strategic Archetypes Approach to Understanding the Blockchain," available at *https://aisel.aisnet.org/icis2016/Crowdsourcing/Presentations/6/*.

Williamson, O. E. 1975. "Markets and Hierarchies," New York, NY: The Free Press.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. 2017. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings of the International Congress on Big Data (BigData Congress)*, IEEE, pp. 557-564.

Ziolkowski, R., Miscione, G., and Schwabe, G. 2018. "Consensus through Blockchains: Exploring Governance across Inter-Organizational Settings," available at: *https://aisel.aisnet.org/icis2018/governance/Presentations/10/*.

Ziolkowski, R., Parangi, G., Miscione, G., and Schwabe, G. 2019. "Examining Gentle Rivalry: Decision-Making in Blockchain Systems," in *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS),* IEEE.

Zittrain, J. L. 2006. "The Generative Internet," *Harvard Law Review* (119), pp. 1974-2040.